c. Discovery (Criminal)

(1) A prosecutor is allowed to request any and all applicable digital video files of an incident. Digital video files requested will be made available via a Secured File Transfer Protocol (SFTP) site. If unable to use this site, two physical copies will be provided unless otherwise specified on the video request form—one for the prosecutor and one for the defense, provided by the prosecutor.

(2) A defendant and/or their attorney of record may be allowed to view or receive a copy of a video of an incident in question by submitting a request directly to the Public Disclosure Coordinator (see **PUBLIC RECORDS REQUESTS**).

d. Public Disclosure

(1) In processing requests for disclosure of VHS tapes or digital video recordings made pursuant to the Public Records Act (chapter 42.56 RCW), the Video Coordinator and Public Disclosure Coordinator shall follow department policies and procedures and applicable laws, including RCW 9.73.090.

7. VHS tapes are no longer issued or deployed in the department. However, the district designee shall maintain existing VHS tape recordings in accordance with agency hold notices and laws governing records retention and evidence. When destruction of a VHS tape is appropriate (i.e., retention, hold notice, and evidentiary obligations have been met), the district designee regarding VHS tapes shall document the date of destruction and maintain a record of the disposition of each sequentially numbered video tape for audit purposes. Recorded VHS tapes shall be stored in a locked container/room. Only the Public Disclosure Coordinator and his/her supervisor shall have access to the container/room.

Applies to: All WSP Officers, Risk Management Division
See Also: RCW 9.73.080(1)(c), 9.73.090, Chapters 9.73, 42.52, 42.56 RCW; WSP Policies **Attorney General's Records Hold Notice Requirements, Records Retention, Electronic Records Storage, Employee Access to Electronic Information, Public Records Requests, Inspections**; *Public Disclosure Manual*; *Video Program Standard Operating Procedures Manual*; Report of Training; Recorded Defendant/Witness Statement; Report of Investigation; Video Requests – Discovery, Request for Public Records; Video Request – General

18.00.160 AUTOMATED LICENSE PLATE READERS (ALPR)

I. POLICY

A. ALPR Requests

1. All requests to purchase or use ALPR technology shall be approved by the Chief.

2. Divisions/districts desiring to use ALPR technology shall submit an IOC request providing justification and explaining how it will be used. The request shall include a proposed division/district-specific procedure that complies with the minimum standards of this policy.

B. ALPR Procedures

1. Each division/district using ALPR shall designate a system administrator with responsibilities that include, but are not limited to the following:

   a. Oversee and administer the ALPR program, including the storage and management of ALPR data.

   b. Ensure all operators are trained and approved to operate the ALPR system prior to the system's usage.

   c. Ensure all training is documented.

   d. Ensure ongoing training is provided as needed.

   e. Control access and use of ALPR data according to established guidelines.

2. Prior to taking any action, ALPR hits shall be verified, including a check to ensure the plate was read correctly by the system.

3. Personnel are prohibited from using the ALPR system until properly trained in its use, including operational protocols.

4. Prior to running any ALPR data through the National Crime Information Center (NCIC) or the Washington Crime Information Center (WACIC), operators shall be ACCESS Level 1 certified.

5. ALPR operation and access to ALPR collected data shall be for official agency purposes only.

6. ALPR operators shall meet WSP employee criteria, including polygraph, fingerprints, and background check.

7. No officer shall use, or authorize the use of, the equipment or database records for any non-approved reason.

C. Data Collection and Retention

1. Only trained and approved personnel may access ALPR data.

2. All mobile ALPR data recorded should be downloaded daily, but no later than the officer's next scheduled duty day, or maximum of 72 hours, with supervisor approval.

3. Once the data is transferred, it shall be purged immediately, or as soon as practicable, from the mobile ALPR/laptop.

4. All ALPR data downloaded to the server will be stored no longer than 60 days prior to purging, unless it has become (or it is reasonable to believe that it will become) evidence in a specific

criminal or civil action. In those circumstances, the applicable data shall be downloaded to a compact disk (CD) or other portable storage device and provided to the case officer. It shall be subject to the same logging, handling, and chain of custody requirements as other evidence. Data given to the License Investigation Unit (LIU) databases will no longer be considered ALPR data and will be retained or utilized per the LIU section procedures.

5. All requests for access to stored ALPR data shall be logged and a written request explaining the purpose for the data shall be provided. This information will be maintained in the same manner as criminal history logs.

6. Officers approved to access ALPR data under these guidelines are permitted to access the data when there is an articulable suspicion that the data relates to an investigation in a specific criminal or civil action.

7. Except as otherwise provided by law, all electronic images or data gathered by ALPR is for the exclusive use of law enforcement in the discharge of duties and are not to be made open to the public. Nothing in this policy should be interpreted to limit the use of the electronic images or data for legitimate purposes by prosecutors or others legally permitted to receive evidence under the law.

Applies to: WSP Officers
See Also: --